WHAT IS CLAIMED IS:

1. A universal mobile ID (UMID) system for use in a computer system including a client computer employed by a user and a server computer from which the client computer downloads content via a network, comprising:

a public PIN associated with the client computer; and at least one of:

user-specific information, including at least one of:

user preferences that can be used by the server to filter the content; and

access rights that can be used by the server to limit access of the user to the content; and

device-specific information, including at least one of:

device attributes of the client that can be used by the server to customize the content so that it is suitable for use on the client; and

date of birth (DOB) of the client; at least a subset of the user preferences, access rights and device attributes being dynamically modifiable by any combination of the user and a client program executing on the client computer; and

the public PIN, user-specific information and device-specific information being transmitted to the server by the client to enable the server to appropriately configure the content to be downloaded to the client.

2. The UMID system of claim 1, further comprising:

a secret PIN associated with the client accessible to the client and the server;

wherein the secret PIN is used by the server, when the content is encrypted, to generate a decryption factor with which the client, in conjunction with the secret PIN, can decrypt the encrypted content.

3. The UMID system of claim 2, wherein the secret PIN is stored on both the client and the server at birth.

4. The UMID system of claim 3, wherein:

the secret PIN stored on the client is encrypted prior to storage with an encryption key derived at least partially using biometric information taken from the user.

5. The UMID system of claim 1, wherein the secret PIN is generated by a client security program executing on the client and is transmitted to the server in a secure manner.

6. The UMID system of claim 5, wherein the secret PIN is generated using at least one of:

(1) hardware/software configuration information assumed to be unique for the client;

(2) patterns of bits in selected files stored on the client; and

(3) a set of biometric information associated with the user.

7. The UMID system of claim 6, wherein the biometric information includes at least one of:

handwriting characteristics;

one or more fingerprints;

voice print;

retina pattern; and

typing pattern.

8. The UMID system of claim 6, wherein, when the secret PIN is generated using the biometric information, the secret PIN is not stored on the client.

9. The UMID system of claim 6, wherein the secret PIN is stored on the client in a secure manner.

10. The UMID of claim 9, wherein, when the secret PIN is derived using the biometric information, prior to storage the secret PIN is encrypted with an encryption key derived at least partially using the biometric information.

11. The UMID of claim 1, wherein the public PIN, user-specific information, device-specific information, and date of birth (DOB) are stored on the client at birth.

12. The UMID of claim 1, wherein the public PIN, user-specific information and device-specific information are generated by the server in response to questions answered by the user and then downloaded to the client.

13. The UMID of claim 1, wherein:

the user preferences include:

types of content in which the user is interested;

image type;

color depth;

image scaling;

display attributes;

the access rights include blocking rights; and

the device attributes include:

memory size;

connection speed to the network; and

client device locality.

14. A method for providing digital rights management in an open, networked environment wherein a client computer is employed by a user to download content from a server computer via a network, comprising:

assigning the client a secret PIN;

registering the secret PIN with the server;

assigning the client a universal mobile ID (UMID), which includes:

a public PIN associated with the client computer; and at least one of:

user-specific information, including at least one of:

user preferences that can be used by the server to filter the content; and

access rights that can be used by the server to limit access of the user to the content; and

device-specific information, including at least one of:

device attributes of the client that can be used by the server to customize the content so that it is suitable for use on the client; and

date of birth (DOB) of the client;

associating in the server the secret PIN and the public PIN;

determining content stored on the server to be downloaded to the client;

customizing content to be downloaded to the server using at least a subset of the UMID;

encrypting on the server the content to be downloaded;

downloading the encrypted content to the client; and

decrypting on the client the encrypted content using a decryption key derived from the secret PIN.

15. The digital rights management method of claim 14, further comprising:

associating with a content item a respective content key;

encrypting the content item with the respective content key;

determining from the content key associated with the content to be downloaded and the secret PIN of the user a decryption factor;

the client employing the decryption factor and the secret PIN to derive the decryption key without which the client cannot access the encrypted content.

16. The digital rights management method of claim 14, wherein the secret PIN assigning step comprises setting the secret ID at the time of manufacturing of the client.

17. The digital rights management method of claim 14, wherein the secret PIN assigning step comprises generating the secret PIN using a client security program executing on the client.

18. The digital rights management method of claim 17, wherein the secret PIN generating step comprises generating the PIN as a function of at least one of:

(1) hardware/software configuration information assumed to be unique for the client;

(2) patterns of bits in selected files stored on the client; and

(3) a set of biometric information associated with the user.

19. The digital rights management method of claim 18, wherein the biometric information includes at least one of:

handwriting characteristics;

one or more fingerprints;

voice print;

retina pattern; and

typing pattern.

20. The digital rights management method of claim 14, further comprising storing the secret PIN on the client in a secure manner.

21. The digital rights management method of claim 24, wherein the step of storing the secret PIN on the client in a secure manner comprises:

when the secret PIN is derived using the biometric information, encrypting the secret PIN with an encryption key derived at least partially using the biometric information, neither the encryption key nor an associated decryption key ever being permanently stored on the client, such that, when necessary, the client derives the decryption key and the encryption key using the biometric information.

22. The digital rights management method of claim 14, wherein the UMID assigning step comprises the server generating the public PIN, user-specific information and device-specific information in response to questions answered by the user and then downloading the UMID to the client.

23. The digital rights management method of claim 14, wherein:

the user preferences include:

types of content in which the user is interested;

image type;

color depth;

image scaling;

display attributes;

the access rights include blocking rights; and

the device attributes include:

memory size;

connection speed to the network; and

client device locality.

24. The digital rights management method of claim 14, further comprising the step of:

allowing any combination of the user and a client program to dynamically modify at least a subset of the user preferences, access rights and device attributes.

25. The digital rights management method of claim 24, further comprising:

when the device attributes include memory size, allowing the client program to dynamically modify the memory size in accordance with memory available in the client; and

the server modifying the content accordingly so that the content downloaded from the server fits in the memory available in the client.

26. The digital rights management method of claim 24, further comprising:

when the device attributes include connection speed, allowing the client program to dynamically modify the connection speed in accordance with current speed of client connection to the network; and

the server modifying the content accordingly so that the content downloaded from the server is compatible with the connection speed.

27. The digital rights management method of claim 14, wherein the content is for-pay content, further comprising:

paying the server for the content prior to the downloading step.

28. A secret PIN associated with a client configured to download encrypted content from a server, wherein:

the secret PIN is accessible to the client and the server;

the secret PIN is used by the server to generate a decryption factor with which the client, in conjunction with the secret PIN, can decrypt the encrypted content;

the secret PIN is reliably generated by the client anytime it is needed; and

neither the secret PIN nor data used to generate the secret PIN are stored on the client.

29. The secret PIN of claim 28, wherein the secret PIN is generated by a client security program executing on the client and is transmitted to the server in a secure manner.

30. The secret PIN of claim 29, wherein the secret PIN is generated using a set of biometric information associated with the user.

31. The UMID system of claim 30, wherein the biometric information includes at least one of:

handwriting characteristics;
one or more fingerprints;
voice print;
retina pattern; and
typing pattern.

32. A dynamic, universal mobile ID for use in a client computer configured to download content from a server computer, comprising:
device information that describes configuration of the client;
at least a subset of the device information being dynamically modifiable by the client computer;
the dynamic universal mobile ID being transmitted to the server computer to enable the server computer to customize the content to be downloaded to the client computer;

33. The dynamic, universal mobile ID of claim 32, wherein the subset includes device parameters impacting at least one of:
size of the content that can be stored in client memory;
bandwidth of the content that can be transmitted between the client computer and the server computer;
complexity of the content that can be accessed by the client computer; and
geographic relevance of the content.

34. The dynamic, universal mobile ID of claim 32, wherein the device parameters include at least one of:
network connection speed between the client and server computers;
available network capacity;
processor capability;
available processor capacity;
available client memory;
client geographic position; and
client time zone.

35. The dynamic, universal mobile ID of claim 32, wherein the content is subscription content, further comprising:

subscription information indicating particular types of subscription content;

the server downloading the subscription content as appropriate in a push mode operation.

36. The dynamic, universal mobile ID of claim 35, further comprising:

payment information;

the server charging the client for downloaded subscription content using the payment information.

37. The dynamic, universal mobile ID of claim 35, wherein the server charges the client for downloaded subscription content using payment information forwarded to the server by the server in a separate registration operation.

38. A method for enabling a client computer to download and use encrypted content from a server computer, comprising:

a registration phase, including:

the client transmitting to the server a secret PIN associated with the client computer; and

the server associating with the secret PIN a public PIN associated with the client computer; and

a downloading phase, including:

the client issuing a request to the server for the encrypted content;

the client identifying itself as the source of the request using the public PIN;

the server looking up the secret PIN using the public PIN;

the server generating a decryption factor based on the secret PIN that can be used by the client in conjunction with the secret PIN to decrypt the encrypted content;

the server transmitting the encrypted content and the decryption factor to the client.

39. The method of claim 38, further comprising:

the client deriving a decryption key using the decryption factor and the secret PIN;

the client decrypting the encrypted content using the decryption key.

40. The method of claim 38, wherein:

the encrypted content is for-pay content;

the registration phase includes the client forwarding to the server payment information; and

the downloading phase includes the client authorizing payment for the for-pay content.

41. The method of claim 38, wherein:

the secret PIN is reliably generated by the client anytime it is needed; and

neither the secret PIN nor data used to generate the secret PIN are stored on the client.